IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method for generating an authentication tag for a message that can be used for error correction comprising:

processing a portion of the message using a reversible first function to produce an intermediate result; ~~and~~

processing the intermediate result with a second function to produce the authentication tag; and

encrypting the intermediate result.

2. (Cancelled)

3. (Currently Amended) The method of claim ~~2~~1, further comprising sending the intermediate result to a receiver of the message.

4. (Original) The method of claim 3, further comprising sending the authentication tag to the receiver.

5. (Currently Amended) A method for detecting errors in a message comprising:

receiving at least one message data word and an authentication tag, said authentication tag produced from said at least one message data word according to a nested message authentication code having a reversible inner function;

processing said received at least one message data word according to said nested message authentication code to produce an authentication tag;

determining whether said produced authentication tag is the same as said received authentication tag;

wherein said receiving comprises receiving at least one message data word, an authentication tag, and an intermediate result from said reversible inner function.

6. (Cancelled)

7. (Currently Amended) The method of claim 5, wherein said receiving comprises receiving ~~at least one message data word, an authentication tag, and~~ an encrypted intermediate result from said reversible inner function.

8. (Original) The method of claim 7, further comprising decrypting said encrypted intermediate result if said produced authentication tag is not the same as said received authentication tag.

9. (Original) The method of claim 7, wherein said processing comprises processing said received at least one message data word according to said nested message authentication code to produce an authentication tag and an intermediate result from said reversible inner function.

a'

10. (Original) The method of claim 9, further comprising determining whether said decrypted intermediate result is the same as said produced intermediate result.

11. (Original) The method of claim 10, further comprising correcting an erroneous message data word if said decrypted intermediate result is not the same as said produced intermediate result.

12. (Original) The method of claim 10, wherein said correcting comprises identifying said erroneous message data word using a reverse inner function corresponding to said reversible inner function.

13. (New) A system for detecting errors in a message comprising:

means for receiving at least one message data word and an authentication tag, said authentication tag produced from said at least one message data word according to a nested message authentication code having a reversible inner function;

means for processing said received at least one message data word according to said nested message authentication code to produce an authentication tag;

means for determining whether said produced authentication tag is the same as said received authentication tag;

wherein said receiving comprises receiving at least one message data word, an authentication tag, and an intermediate result from said reversible inner function.

14. (New) The system of claim 13, wherein said receiving comprises receiving an encrypted intermediate result from said reversible inner function.

15. (New) The system of claim 14, further comprising means for decrypting said encrypted intermediate result if said produced authentication tag is not the same as said received authentication tag.

16. (New) The system of claim 14, wherein said processing comprises processing said received at least one message data word according to said nested message authentication code to produce an authentication tag and an intermediate result from said reversible inner function.

17. (New) The system of claim 16, further comprising means for determining whether said decrypted intermediate result is the same as said produced intermediate result.

18. (New) The system of claim 17, further comprising means for correcting an erroneous message data word if said decrypted intermediate result is not the same as said produced intermediate result.

19. (New) The system of claim 17, wherein said correcting comprises identifying said erroneous message data word using a reverse inner function corresponding to said reversible inner function.

20. (New) A computer program product embodied on a computer readable medium for detecting errors in a message comprising:

computer code for receiving at least one message data word and an authentication tag, said authentication tag produced from said at least one message data word according to a nested message authentication code having a reversible inner function;

computer code for processing said received at least one message data word according to said nested message authentication code to produce an authentication tag;

computer code for determining whether said produced authentication tag is the same as said received authentication tag;

wherein said receiving comprises receiving at least one message data word, an authentication tag, and an intermediate result from said reversible inner function.

21. (New) The computer program product of claim 20, wherein said receiving comprises receiving an encrypted intermediate result from said reversible inner function.

22. (New) The computer program product of claim 21, further comprising computer code for decrypting said encrypted intermediate result if said produced authentication tag is not the same as said received authentication tag.

23. (New) The computer program product of claim 21, wherein said processing comprises processing said received at least one message data word according to said nested message authentication code to produce an authentication tag and an intermediate result from said reversible inner function.

24. (New) The computer program product of claim 23, further comprising computer code for determining whether said decrypted intermediate result is the same as said produced intermediate result.

25. (New) The computer program product of claim 24, further comprising computer code for correcting an erroneous message data word if said decrypted intermediate result is not the same as said produced intermediate result.

26. (New) The computer program product of claim 24, wherein said correcting comprises identifying said erroneous message data word using a reverse inner function corresponding to said reversible inner function.